



mosquitto-tls man page

Name

mosquitto-tls — Configure SSL/TLS support for Mosquitto

Description

mosquitto provides SSL support for encrypted network connections and authentication. This manual describes how to create the files needed.

Note

It is important to use different certificate subject parameters for your CA, server and clients. If the certificates appear identical, even though generated separately, the broker/client will not be able to distinguish between them and you will experience difficult to diagnose errors.

Generating certificates

The sections below give the openssl commands that can be used to generate certificates, but without any context. The asciicast at <https://asciinema.org/a/201826> gives a full run through of how to use those commands.

Certificate Authority

Generate a certificate authority certificate and key.

```
openssl req -new -x509 -days <duration> -extensions v3_ca -keyout  
o ca.key -out ca.crt
```

Server

Generate a server key.

- `openssl genrsa -des3 -out server.key 2048`

Generate a server key without encryption.

- `openssl genrsa -out server.key 2048`

Generate a certificate signing request to send to the CA.

- `openssl req -out server.csr -key server.key -new`

Note

When prompted for the CN (Common Name), please enter either your server (or broker) hostname or domain name.

Send the CSR to the CA, or sign it with your CA key:

- `openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key`
- `-CAcreateserial -out server.crt -days <duration>`

Client

Generate a client key.

- `openssl genrsa -des3 -out client.key 2048`

Generate a certificate signing request to send to the CA.

- `openssl req -out client.csr -key client.key -new`

Send the CSR to the CA, or sign it with your CA key:

- `openssl x509 -req -in client.csr -CA ca.crt -CAkey ca.key`
- `-CAcreateserial -out client.crt -days <duration>`

See Also

[mosquitto\(8\)](#) , [mosquitto-conf\(5\)](#)

Author

Roger Light <roger@atchoo.org>

[Eclipse Home](#) [Market Place](#) [Eclipse Live](#) [Eclipse Planet](#) [Eclipse
Security](#) [Privacy Policy](#) [Terms of Use](#) [Copyright Agent](#) [Legal](#)